# CYBERSECURITY (SEC)

**SEC 010 Lower Div Transfer Course Work Credits: 1-12**
**Course Description:** This course is an undergraduate lower division course. It is assigned during the review of transfer transcripts and the transcript evaluation process. Transfer courses that do not have a MWSU course equivalency in this department may receive this subject code and course number.

**SEC 030 Upper Div Transfer Course Work Credits: 1-12**
**Course Description:** This course is an undergraduate upper division course. It is assigned during the the review of transfer transcripts and the transcript evaluation process. Transfer courses that do not have a MWSU course equivalency in this department may receive this subject code and course number.

**SEC 100 Introduction to Cybersecurity Credits: 3**
**Typically Offered:** Spring (odd-numbered years).
**Course Description:** This course covers the fundamental issues and principles of computer-and-network security through studying theory and through hands-on assignments and lab exercises. The course will look at the capabilities of modern cryptographic systems and the NIST Cybersecurity Framework. Students will learn how to secure a computer, or a network, by analyzing its security requirements and applying common techniques to enforce them. **Prerequisite(s):** ACT 101.

**SEC 200 Computer Hardware and Peripherals Credits: 3**
**Typically Offered:** Fall (odd-numbered years).
**Course Description:** This course explores the fundamentals of computer hardware, including processors, memory storage devices, and input/output peripherals. Students will be introduced to basic skills required to troubleshoot, maintain, and repair computes. Emphasis will be placed on selecting, assembling, and maintaining computer systems and peripherals.

**SEC 260 Introduction to Digital Forensics Credits: 3**
**Typically Offered:** Spring (even-numbered years).
**Course Description:** An overview of digital forensics and computer-related issues facing government and businesses. Specific focus on forensic examinations and methodologies used in the field. Students will also explore the legal, ethical, and technical challenges involved in collecting and preserving digital evidence. **Prerequisite(s):** SEC 100.

**SEC 305 Applied Cryptography Credits: 3**
**Typically Offered:** Fall (even-numbered years).
**Course Description:** This course provides students with a comprehensive understanding of cryptographic algorithms, protocols, and techniques essential for securing modern applications. It emphasizes both foundational concepts and recent advancements in applied cryptography, equipping students to design, implement, and apply cryptographic solutions effectively in real-world scenarios. The curriculum focuses on both theoretical principles and practical implementations critical to security-critical systems. **Prerequisite(s):** CSC 386 and a grade of C or higher in MAT 110/110E or higher MAT class.

**SEC 310 Securing and Defending Networks Credits: 3**
**Typically Offered:** Fall (even-numbered years).
**Course Description:** In this course, students will master their skills in securing an endpoint, which can be a computer or an IoT device, through hardening its software components, physical/software interfaces, and the networks and endpoints will be discussed together with the threats that exploit those vulnerabilities, the attach vectors for various hardware and software components, and countermeasures that thwart the attacks. Students will also learn about documenting for the purpose of securing computer systems and networks. **Prerequisite(s):** SEC 100.

**SEC 325 Cybercrime Credits: 3**
**Typically Offered:** Fall (odd-numbered years).
**Course Description:** This course explores cybercrime and computer intrusions, focusing on prevention, detection, and investigation, particularly in workplace settings. Students will study crimes like hacking, fraud, and identity theft while gaining hands-on experience with forensic tools, digital evidence collection, and OSINT techniques. The course prepares students to handle incidents, mitigate risks, and secure critical assets, equipping them for careers in cybersecurity, forensics, or corporate security. **Prerequisite(s):** SEC 310.

**SEC 335 Network and Endpoint Security I Credits: 3**
**Typically Offered:** Departmental Discretion.
**Course Description:** This course will introduce students to system security in terms of securing software components, physical/software interfaces, and networks. Vulnerabilities of common network protocols, threats that exploit those vulnerabilities, and attack models will be discussed. Students will learn about the basics of software security, software vulnerabilities, and cloud administration. Students will learn the underlying security theory and will gain hands on experience through lab exercises. **Prerequisite(s):** SEC 100.

**SEC 350 Emerging Technologies in Cybesecurity Credits: 3**
**Typically Offered:** Spring (odd-numbered years).
**Course Description:** This course focuses on how organizations adopt new technologies, preparing for associated risks and challenges. Students will compare evolving technologies to address an organization's security needs and explore the principles necessary for secure network operations. By the end of the course, students will understand the strategies required to implement new technologies while maintaining robust cybersecurity practices. **Prerequisite(s):** SEC 100.

**SEC 360 Laws and Ethics in Cybersecurity and AI Credits: 3**
**Typically Offered:** Spring (even-numbered years).
**Course Description:** This course explores the legal frameworks and ethical considerations surrounding cybersecurity and emerging technologies, with a focus on AI. Students will examine privacy laws, cybercrime regulations, and compliance standards while addressing the ethical challenges involved in data protection and surveillance. Topics include the role of AI in cybersecurity, ethical dilemmas such as bias and accountability, and the application of frameworks like the trolley problem to real-world scenarios. Through case studies and hands-on projects, students will develop the skills to navigate complex legal landscapes and make informed, ethical security decisions. **Prerequisite(s):** SEC 100.

**SEC 380 Critical Infrastructure Threats and Security Credits: 3**
**Typically Offered:** Spring (odd-numbered years).
**Course Description:** This course examines major threats, protection strategies, and technologies related to critical infrastructure sectors, including telecommunications, energy, banking and finance, transportation, supply chains, industrial control systems (ICS), operational technology (OT), and emergency services. Emphasis is placed on identifying vulnerabilities and implementing security measures to safeguard essential services. **Prerequisite(s):** SEC 100.

**SEC 400 Cyber Investigations Credits: 3**
**Typically Offered:** Spring (even-numbered years).
**Course Description:** This course presents students with concepts and processes required to develop and execute an incident response and forensic investigation plan. The student will experiment with basic understanding of incident response capabilities, evidence handling procedures, and remediation. Students will test security tools and technologies through hands-on practical exercises and research presentations. This course builds foundational knowledge for incident response and network forensics practitioners. **Prerequisite(s):** SEC 310.

**SEC 415 Data Security and Identity Management Credits: 3**
**Typically Offered:** Departmental Discretion.
**Course Description:** This course will cover techniques used to protect data from unauthorized access or corruption, and techniques used to identify, authenticate, and authorize individuals or groups to access protected resources. Students will work with open-source tools for cryptography and identity management. **Prerequisite(s):** SEC 100.

**SEC 425 Ethical Hacking Credits: 3**
**Typically Offered:** Spring (odd-numbered years).
**Course Description:** This course will cover how to identify different vulnerabilities from an attacker's point of view, what they might do with these vulnerabilities, and what measures you can take to mitigate these risks. Students will gain practical skills through red-team exercises and penetration labs. **Prerequisite(s):** SEC 310.

**SEC 435 Network and Endpoint Security II Credits: 3**
**Typically Offered:** Departmental Discretion.
**Course Description:** In this course, students will master their skills in securing an endpoint, which can be a computer or an IoT device, through hardening its software components, physical/software interfaces, and the networks and endpoints will be discussed together with the threats that exploit those vulnerabilities, the attach vectors for various hardware and software components, and countermeasures that thwart the attacks. Students will also learn about documenting for the purpose of securing computer systems and networks. **Prerequisite(s):** SEC 335.

**SEC 445 Security Program Governance Credits: 3**
**Typically Offered:** Fall (odd-numbered years).
**Course Description:** This course introduces the development and management of cybersecurity programs within organizations. Governance frameworks and regulations will be studied through development of policy, implementation of controls and audits, analysis of risks, and response to simulated incidents. Students will gain skill with management tools, analyze security concerns with employees and vendors, and implement communication strategies with a variety of stakeholders. **Prerequisite(s):** SEC 100.

**SEC 450 Independent Research/Project Credits: 1-3**
**Typically Offered:** Departmental Discretion.
**Course Description:** Investigation of a research problem, project, or topic on an individual conference basis. May be repeated for credit.

**SEC 455 Cyberlaw and Investigations Credits: 3**
**Typically Offered:** Departmental Discretion.
**Course Description:** This course introduces the US and international laws on cybersecurity, including law related to privacy, data security, crime, and intellectual property. Students will also explore the implications of culture and international agreements on policy and critical infrastructure. Students will learn the essentials of computer investigations through the application of forensic tools. **Prerequisite(s):** SEC 100.

**SEC 490 Cybersecurity Career Preparation Credits: 1**
**Typically Offered:** Fall (even-numbered years).
**Course Description:** In this course students will begin applying their MWSU education towards building a career in Cybersecurity. Students will learn how to navigate a career path in IT, explore alternative career paths, and explore opportunities for continuing education and professional development. Students will develop application materials and attempt entrance, exit, and/or certification exams in preparation for graduation, applying to jobs, and applying to graduate schools. **Prerequisite(s):** Admission to the Cybersecurity program.

**SEC 495 Cybersecurity Capstone Credits: 3**
**Typically Offered:** Spring (even-numbered years).
**Course Description:** This is the capstone course for the Cybersecurity degree students. The capstone course is used to research, document and implement current and advanced IT topics using knowledge and skills developed from networking courses. **Prerequisite(s):** Credit or concurrent enrollment in SEC 490.